

# Disaster Recovery

## Putting Your Company Back in Business

By Jack Carr

**T**hink of the chilling images of papers fluttering to the sidewalk in lower Manhattan as the World Trade Center towers collapsed. Beyond the obvious tragedy of the many lives lost, how much business knowledge was destroyed that morning? If your company had been in those buildings, how long would it have taken to gather your employees, relocate them to a new facility, reconnect the phones and computers and resume business?

“Disasters” on a smaller scale can be just as devastating. Ninety percent of businesses that experience an interruption – even a non-cataclysmic one – close within two years, according to the University of Texas Center for Research on Information Systems. Many businesses that experience a disruption never reopen.

### Are we at risk?

If the term “disaster” sounds like something that couldn’t happen to you, you’re not alone. Sixty percent of businesses have inadequate measures in place to protect the company following an unexpected interruption.

Many business owners feel it’s too expensive to implement a disaster recovery plan because they feel the cost of replicating the business infrastructure is greater than the risk of disaster. However, it costs 15 times more to recover from a disaster without a plan than to execute a properly planned recovery strategy, according to the Federal Emergency Management Association (FEMA).

Disasters come in all shapes and sizes, so be prepared for anything that could cut you off from your suppliers, customers and employees. Tornadoes, floods and other acts of God happen everywhere, and you don’t have to be a target of terrorist activities to find yourself in the dark when the power company accidentally cuts an essential cable to your building.

To develop a plan, first define a disaster for your business. If the phones were unavailable or the power was interrupted for as little as an hour, how much would it impact your profits for the quarter? If your building burned down or flooded or a tornado wiped away your facility, are your records backed up at an off-site location that you can access quickly from another computer? Other examples of business misadventures include lack of water or chemical spills that require evacuation of the building, loss of computer functionality or disruption of computer services – either because your server goes down or someone has hijacked your files. If hackers compromised your data files, how fast could you regain control?

### Business continuity

Disaster planning comes down to this question: How long will it take your customers to move to your competitors if they can’t reach you or if your computer server goes down and your employees can’t access company files?



Jack Carr

A good disaster recovery plan focuses on two things: 1) disaster prevention, such as security safeguards and backup systems; and 2) business continuity, or doing whatever it takes to keep your employees in touch at all times with your customers so they won’t stray during an unexpected down time.

A realistic disaster recovery plan balances the cost of replicating your essential systems against the time frame you can afford to be inaccessible to your customers. Essential systems include data (on internal networks as well as data available to your customers and suppliers via the Internet) and telecommunications, such as phones, voice mail and call center services.

Your plan should focus on restoring essential systems as quickly as possible. Like a good insurance policy, it should cost enough to save you money when disaster strikes, but the cost shouldn’t be a burden to your day-to-day operations.

### Bouncing back

To implement an effective disaster recovery plan, think in terms of “operations resiliency” or your ability to get the business back to a level to serve your customers. The plan should ensure business continuity at a price that makes sense given realistic risks.

For example, a local delivery company that relied on a Global Positioning System to monitor deliveries critical to business clients needed to relocate its computer servers to another facility following a severe storm. IQuest provided co-location space in our data center, helped transport servers and got them hooked back up quickly. The GPS system was back online within one hour, mitigating the impact of the disaster on their bottom line.

You can put a contingency or disaster recovery plan into effect over a period of years, securing essential services first and adding additional security measures as the business grows or changes. A comprehensive planning document identifies all possible risks and opportunities, establishes processes to prevent ill effects and maximize beneficial ones, and outlines a process of business continuation or recovery from a disaster as quickly and effectively as possible.

### INFORMATION LINK

**Author:** Jack Carr is the COO and a managing partner in IQuest Internet LLC, which provides state-of-the-art Internet access and comprehensive e-commerce services from its data center located in downtown Indianapolis. Carr can be contacted at (317) 726-6767 or e-mail: [jcarr@iquest.net](mailto:jcarr@iquest.net)